

CLAIMS:

- Sub B1
1. An encryption method wherein at least one cryptographic sub-operation $y_i = f_i(x_i, k_i)$ is performed on data x_i, k_i which are digitally stored as data bit words, the relevant result or intermediate results y_i being digitally stored or buffered as data bit words, characterized in that
 - 5 at option at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i is bit-wise complemented to \bar{x}_i, \bar{k}_i and/or \bar{y}_i or not, depending on a control signal r_i which is based on random numbers.
 2. An encryption method as claimed in Claim 1,
 - 10 characterized in that one or more XOR (EXCLUSIVE OR) combinations are formed during the cryptographic sub-operations.
 3. An encryption method as claimed in Claim 1 ~~or 2~~,
 - 15 characterized in that the data contain cryptographic keys and/or operands.
 4. An encryption method as claimed in ~~one of the preceding Claims~~ ¹,
 - 20 characterized in that intermediate results y_i are buffered in a register R_i between the execution of successive cryptographic sub-operations and are used as an operand x_{i+1} for the subsequent cryptographic sub-operations.
 5. An encryption method as claimed in ~~one of the preceding Claims~~ ¹,
 - 25 characterized in that a bit series $x_{i+1} = y_i$ derived from the intermediate result y_i of a preceding sub-operation i is bit-wise complemented to \bar{x}_{i+1} for a subsequent-operation $i+1$ if the data x_i, k_i of the preceding sub-operation i were bit-wise complemented.

6. An encryption method as claimed in ~~one of the preceding Claims~~ characterized in that during the bit-wise complementary operation at least one bit value, notably the even bit values, the odd bit values or all bit values, of a data bit word x_i , k_i or y_i are inverted.

7. An encryption method as claimed in ~~one of the preceding Claims~~ characterized in that bit values or bit addresses of a data bit word x_i , k_i or y_i are inverted by means of an XOR operation (EXCLUSIVE OR operation) during the bit-wise complementary operation.

8. An encryption device which includes a processor and registers R_i (14, 16), the processor performing at least one cryptographic sub-operation $y_i = f_i(x_i, k_i)$ (10, 12) on operands x_i , k_i which are digitally stored as data bit words in the registers R_i (14, 16) of the encryption device, the relevant result or intermediate result y_i being digitally stored or buffered as data bit words in the registers R_i (14, 16) of the encryption device, characterized in that there are provided at least one inverter (18 to 28; 30) which can be controlled by a control signal r_i and serves for at least one of the data x_i , k_i and/or the result or at least one intermediate result y_i , a random number generator which generates random numbers, as well as a device for generating the control signal r_i on the basis of the random numbers, the controllable inverter (18 to 28; 30) either, in dependence on the control signal r_i , converting the bit series x_i , k_i or y_i into their bit-wise complement \bar{x}_i , \bar{k}_i and \hat{y}_i , respectively, or leaving them unchanged.

9. An encryption device as claimed in Claim 8, characterized in that at least one register (R_i (14, 16) is succeeded by an inverter (26, 28; 30) which receives the same control signal r_i as the inverter (18, 20) for the data x_i , k_i which precedes the i^{th} sub-operation (10, 12).

10. An encryption device as claimed in Claim 9, characterized in that

the inverter (26, 28) succeeding a register R_i (14, 16) of the i^{th} sub-operation (10, 12) is combined with an inverter (20) for input data x_{i+1} which precedes the subsequent $(i+1)^{\text{th}}$ sub-operation (12).

- 5 11. An encryption device as claimed in Claim 10, characterized in that the combined inverter (30) receives the control signal r_i of the preceding i^{th} sub-operation (10) as well as the control signal r_{i+1} of the subsequent $(i+1)^{\text{th}}$ sub-operation (12).

- A 10 12. An encryption device as claimed in ^{claim 11} ~~one of the Claims 8 to 11~~, characterized in that the data contain cryptographic keys and/or operands.

- A 15 13. An encryption device as claimed in ~~one of the Claims 8 to 12~~, characterized in that between a preceding i^{th} sub-operation (10) and a subsequent $(i+1)^{\text{th}}$ sub-operation (12) a register R_i (14, 16) stores an intermediate result y_i of the preceding i^{th} sub-operation (10) and forwards this intermediate result as an input value x_{i+1} to the subsequent $(i+1)^{\text{th}}$ sub-operation (12).

- A 20 14. An encryption device as claimed in ~~one of the Claims 8 to 13~~, characterized in that the bit-wise complementary operation inverts at least one bit value, notably the even bit values, the odd bit values or all bit values, of a data bit word x_i , k_i or y_i .

009250" 50E59560

[illegible]

	10	i^{th} sub-operation
	12	$(i+1)^{\text{th}}$ sub-operation
5	14	register R_i
	16	register R_{i+1}
	18	controllable inverter for x_i
	20	controllable inverter for x_{i+1}
	22	controllable inverter for k_i
10	24	controllable inverter for k_{i+1}
	26	controllable inverter for y_i
	28	controllable inverter for y_{i+1}
	30	combined inverter